UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,676	06/12/2006	John Alan Gervais	PU030342	4964

24498 7590 03/04/2009
Robert D. Shedd
Thomson Licensing LLC
PO Box 5312
PRINCETON, NJ 08543-5312

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2431	
MAIL DATE	**DELIVERY MODE**
03/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/582,676	**Applicant(s)** GERVAIS ET AL.
	Examiner ARAVIND K. MOORTHY	**Art Unit** 2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 November 2008* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 14 November 2008.

2. Claims 1-13 are pending in the application.

3. Claims 1-13 have been rejected.

Response to Amendment

4. The examiner approves of the new abstract. The new abstract commences on a separate sheet. The examiner withdraws the objection made to the specification.

5. The examiner approves of the new drawings. The new drawings no longer contain the label "SUBSTITUTE SHEET". The examiner withdraws the objection made to the drawings.

Response to Arguments

6. Applicant's arguments filed 14 November 2008 have been fully considered but they are not persuasive.

On page 12, the applicant argues, with regard to claim 1, that Marsh fails to disclose ore remotely suggest "a removable digital memory including a port at which digital information stored on said memory can be accessed.

The examiner respectfully disagrees. Marsh discloses that system 220 is coupled to a smart card reader 248 (e.g., via a standard connection such as a USB connection), allowing descrambling and encrypting module 222 to communicate with smart card reader 248 via content protection controller module 238. Smart card 246 can be coupled to smart card reader 248 in a variety of different manners, including physical touching (e.g., electrical contacts of smart card reader 248 being placed in physical contact with electrical contacts of smart card 246) or without such physical contact (e.g., a wireless connection, such as infrared, radio frequency, etc.). Smart card 246 is an integrated circuit card (ICC) which is typically the size of a standard credit card and which is capable of storing data and performing some processing. In one implementation, smart card 246 complies with the ISO 7816 standard. Although discussed herein as a smart card, other types of portable integrated circuit (IC) devices can alternatively be used.

On page 13, the applicant argues, regarding claim 1, Marsh does not teach or suggest a device comprising, inter alia, "memory for storing first conditional access data and at least one content encryption key".

The examiner respectfully disagrees. Marsh discloses conditional access data in the form of a certificate. Marsh discloses that the smart card holds a pair of keys. The smart card transmits to the module a key to be used for encryption.

On page 14, the applicant argues, regarding claim 6, that Marsh does not teach or suggest an access card comprising, inter alia, "memory, following authentication of said card with a destination device, is updated to store a public key of a public/private key pair stored in said destination device".

The examiner respectfully disagrees. Marsh discloses that authentication takes place between the module and the smart card using a challenge. After authentication of the smart card takes place, the module transmits the public key to the smart card for decryption of data.

On page 15, the applicant argues, regarding claim 8, that Marsh does not disclose or suggest a digital information destination device comprising, inter alia, "memory preloaded with at least a second stored User Certificate and mutually corresponding private and public encryption keys associated with said destination device".

The examiner respectfully disagrees. The module receives a certificate from the certificate authority consisting of a public/private key pair. The certificate sent from the certificate authority is used to verify the certificate received from the smart card.

On page 16, the applicant argues, regarding claim 9, Marsh fails to teach or suggest a "source device having a removable digital memory containing information accessible to the source device" as recited in the preamble of the claim 9. The applicant argues that Marsh fails to teach a method of "encrypting said information stored in said removable digital memory using at least one content encryption key stored in said source device" as recited in the body of claim 9. The applicant argues, regarding claim 10, Marsh fails to disclose “providing a source device having a removable digital memory”. The applicant argues that Marsh does not teach or suggest that the source device “includes a first Conditional Access Certificate” nor does Marsh suggest “providing a destination device having a second stored User Certificate and also including mutually corresponding private and public encryption keys associated with said destination device”.

The examiner respectfully disagrees. In response to applicant's arguments, the recitation "source device having a removable digital memory containing information accessible to the source device" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). Marsh discloses the data to be encrypted is passed via the secure communication channel to smart card 246. Processor 262 executes the encryption algorithm to encrypt the data based on the private key of key pair 270 (and household identifier 268, if separate from the private key) and returns the encrypted data to module 222 via the secure communication channel. This alternative has the benefit of smart card 246 not divulging its private key to module 222. Marsh discloses that system 220 is coupled to a smart card reader 248 (e.g., via a standard connection such as a USB connection), allowing descrambling and encrypting module 222 to communicate with smart card reader 248 via content protection controller module 238. Smart card 246 can be coupled to smart card reader 248 in a variety of different manners, including physical touching (e.g., electrical contacts of smart card reader 248 being placed in physical contact with electrical contacts of smart card 246) or without such physical contact (e.g., a wireless connection, such as infrared, radio frequency, etc.). Smart card 246 is an integrated circuit card (ICC) which is typically the size of a standard credit card and which is capable of storing data and performing some processing. In one implementation, smart card 246 complies with the ISO 7816 standard. Although discussed herein as a smart card, other types of portable integrated circuit (IC) devices can alternatively be used. As discussed above, Marsh discloses that the module receives a certificate from the certificate authority with corresponding public/private key pair.

On page 17, the applicant argues, regarding claim 10, Marsh does not teach or suggest a method which includes "placing the access card in said access card port of said destination device" for authentication and “writing said public encryption key from said destination device to said access card” prior to placing the access card in the source device of the media. The applicant argues, regarding claim 13, Marsh does not disclose or suggest an "access card comprising: a memory having at various times at least first, second and third states".

The examiner respectfully disagrees. Marsh discloses that system 220 is coupled to a smart card reader 248 (e.g., via a standard connection such as a USB connection), allowing descrambling and encrypting module 222 to communicate with smart card reader 248 via content protection controller module 238. Smart card 246 can be coupled to smart card reader 248 in a variety of different manners, including physical touching (e.g., electrical contacts of smart card reader 248 being placed in physical contact with electrical contacts of smart card 246) or without such physical contact (e.g., a wireless connection, such as infrared, radio frequency, etc.). Marsh discloses that authentication takes place between the module and the smart card using a challenge. After authentication of the smart card takes place, the module transmits the public key to the smart card for decryption of data. As to the first state, as discussed above, Marsh discloses a second certificate received from a certificate authority and a first certificate stored on the smart card. As to the second state, authentication takes place at the module by comparing the certificate stored on the card and the certificate received from the certificate authority. As to the third state, Marsh discloses the smart card is authenticated using challenge data.

On page 18, the applicant argues, with reference to claim 6, Marsh does not make any suggestion that any information on the smart card is changed and/or updated.

The examiner respectfully disagrees. Marsh discloses that authentication takes place between the module and the smart card using a challenge. After authentication of the smart card takes place, the module transmits the public key to the smart card for decryption of data.

On page 19, the applicant argues, regarding claims 2, 3, 7, 11 and 12, Roskind does not disclose systems and methods for encryption and decryption of media content. The applicant argues that Roskind only teaches systems and methods for authentication of certificates and does not remotely suggest any of the deficiencies of Marsh.

The examiner asserts that Roskind was not used to disclose any system or method for encryption and decryption of media content. Marsh was used to disclose those features. As discussed above, there are no deficiencies in the Marsh reference.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 4-6, 8-10 and 13 are rejected under 35 U.S.C. 102(e) as being anticipated by Marsh U.S. Patent No. 7,080,039 B1.

As to claim 1, Marsh discloses a device, comprising:

> a removable digital memory including a port at which digital information stored on the memory can be accessed (i.e. set-top box 242 provides received content 240 that satisfies the conditional access scheme to descrambling and encrypting module 222 via a coupling 244. Set-top box 242 scrambles the content it passes to module 222 in order to prevent a malicious user from tapping into the signal passed between box 242 and module 222 and inappropriately using the

content. Coupling 244 can be any of a variety of communications mechanisms, including both wired and wireless. In one implementation, coupling 244 is a USB (Universal Serial Bus) or IEEE 1394 connection) [column 7, lines 11-25];

a memory for storing first conditional access data and at least one content encryption key (i.e. Certificate 276 is a certificate that is digitally signed by a trusted licensing authority (also referred to as a certificate authority or certifying authority) testifying that the smart card 246 is authentic. Certificate 276 includes the public key of key pair 270, the public key of the licensing authority, and the above testimony, and is digitally signed by the licensing authority using the private key of the licensing authority. This digitally signed certificate allows module 222, knowing the public key of the licensing authority, to verify that the certificate that is presented by smart card 246 was indeed digitally signed by the licensing authority.) [column 9, lines 57-67];

a second port for receiving user certificate data and a first key of a key pair contained in an access card (i.e. System 220 is coupled to a smart card reader 248 (e.g., via a standard connection such as a USB connection), allowing descrambling and encrypting module 222 to communicate with smart card reader 248 via content protection controller module 238. Smart card 246 can be coupled to smart card reader 248 in a variety of different manners, including physical touching (e.g., electrical contacts of smart card reader 248 being placed in physical contact with electrical contacts of smart card 246) or without such physical contact (e.g., a wireless connection, such as infrared, radio frequency, etc.). Smart card 246 is an integrated circuit card (ICC) which is typically the size of a standard credit card and which is capable of storing data and performing some processing. In one implementation, smart card 246 complies with the ISO 7816 standard. Although discussed herein as a smart card, other types of portable integrated circuit (IC) devices can alternatively be used.) [column 8, lines 6-22]; and

a processor responsive to the user certificate data received on the second port for authenticating the received certificate data based on the first conditional access data stored in the memory (i.e. receiving the certificate, module 222 verifies that the licensing authority is itself trustworthy. Module 222 verifies that the licensing authority is trustworthy by establishing a "chain" of one or more certificates ranging from the licensing authority up to a root certificate. System 220 maintains a root certificate for each licensing authority that system 220 trusts. Each root certificate is a self-signed certificate that is implicitly trusted by system 220. Upon receipt of the smart card certificate 276, module 220 attempts to establish a chain of certificates from the certificate 276 up to one of the trusted root certificates. This chain may include one or more "intermediate" certificates. Each certificate in the chain will have a "parent" certificate that can cryptographically verify the authenticity of the certificate (e.g., by being digitally signed by the parent). Eventually, the chain leads back to a parent certificate that is one of the trusted root certificates. If such a certificate chain can be established by module 222, then the licensing authority is considered trustworthy. However,

> if such a certificate chain cannot be established, then the licensing authority is not considered trustworthy and module 222 will not descramble and encrypt the media content.) [column 10, lines 22-43], the processor, upon the authentication, encrypting information stored in the removable digital memory using the at least one content encryption key, to thereby provide encrypted information in the removable digital memory, the processor operable for encrypting the content encryption key using the first encryption key received on the second port and outputting the encrypted content encryption key to enable access of the encrypted information stored on the removable digital memory by an external device (i.e. The media is encrypted based on smart card 246, thereby requiring smart card 246 to be present in order to decrypt and render the stored content. This decryption and rendering can be performed by any system 220 to which smart card 246 is in communication (e.g., plugged into), such as the system 220 that recorded the content or a system 220 at a friend's house if smart card 246 is taken to the friend's house. Alternatively it can be a physically different smart card, but only if that smart card has the same household identifier stored (securely) inside.) [column 14, lines 15-25].

As to claim 4, Marsh discloses that the first key is a public key of a public/private key pair [column 9, lines 6-8].

As to claim 5, Marsh discloses that the access card is inserted into a slot of the device [column 8, lines 6-22].

As to claim 6, Marsh discloses an access card for enabling secure accessing of digital information stored on a removable memory, the access card comprising:

a memory having stored therein a first conditional access certificate and a second conditional access certificate (i.e. The certificate can be digitally signed by the licensing authority applying a conventional encryption algorithm along with its private key to the certificate to generate a digital signature. This digital signature is forwarded to module 222 along with the certificate. The recipient can decrypt the digital signature using the licensing authority's public key and compare the decrypted certificate to the received certificate. If the two certificates match, then the recipient is ensured that the licensing authority did in fact sign the certificate and that the certificate has not been altered since it was signed. Alternatively, rather than applying an encryption algorithm to the certificate itself, the digital signature may be generated by applying the encryption algorithm to a hash value generated based on the certificate and a known hash function. The digital signature can then be verified by module 222 applying the known hash function to the received certificate and comparing this generated hash value to the decrypted digital signature. If the two hash values match, then module 222 is ensured that the licensing authority did in fact sign the certificate and that the certificate has not been altered since it was signed.) [column 10, lines 1-21];

means for authenticating first and second conditional access certificates with respective first and second certificate data stored on respective destination and source devices [column 10, lines 1-21];

the memory, following authentication of the card with a destination device, being updated to store a public key of a public/private key pair stored in the destination device [column 10, lines 52-61]; and

a processor operable for, upon authentication of the card with a source device, controlling transmission of the public key to the source device, wherein, in response thereto, the memory being updated to store encrypted data comprising a first key encrypted using the public key, the first key also being used to encrypt information on the removable memory at the source device, whereby communication of the encrypted data to the destination device enables decryption of the data using the private key to recover the first key, to thereby decrypt encrypted information in the removable memory (i.e. The media is encrypted based on smart card 246, thereby requiring smart card 246 to be present in order to decrypt and render the stored content. This decryption and rendering can be performed by any system 220 to which smart card 246 is in communication (e.g., plugged into), such as the system 220 that recorded the content or a system 220 at a friend's house if smart card 246 is taken to the friend's house. Alternatively it can be a physically different smart card, but only if that smart card has the same household identifier stored (securely) inside.) [column 14, lines 15-25].

As to claim 8, Marsh discloses a digital information destination device comprising:

a digital information input port (i.e. set-top box 242 provides received content 240 that satisfies the conditional access scheme to descrambling and encrypting module 222 via a coupling 244. Set-top box 242 scrambles the content it passes to module 222 in order to prevent a malicious user from tapping into the signal passed between box 242 and module 222 and inappropriately using the content. Coupling 244 can be any of a variety of communications mechanisms, including both wired and wireless. In one implementation, coupling 244 is a USB (Universal Serial Bus) or IEEE 1394 connection) [column 7, lines 11-25];

a digital information decoder coupled to the digital information input port for decoding digital information encoded with a content encoding key, when the content encoding key is available, to thereby produce unencoded digital information (i.e. The encrypted content is also provided to MPEG decoder module 234. MPEG decoder module 234 decodes (e.g., decompresses) the encoded content (which is encoded in an MPEG format in the illustrated example). Module 234 decrypts the encrypted content prior to decoding the media content, and outputs the decoded content to content renderer module 236. Module 234 can, after decoding the media content, optionally encrypt the decoded content. Whether module 234 encrypts the decoded content is dependent on whether a secure communication channel exists between modules 234 and 236. If there is a secure communication channel (e.g., the modules 234 and 236 are on the same expansion card within system 220, or are within the same display device), then encryption is not necessary. Content renderer module 236 renders the media content via rendering device 294. Although illustrated as a single decoder module 234 and a single renderer module 236, multiple such modules may be included (e.g., one for each type of media content, such as one for audio content and one for video content). Additionally, multiple rendering devices may be included (e.g., one for visual content and another for audio content) [column 12 line 65 to column 13 line 19];

memory preloaded with at least a second stored User Certificate and mutually corresponding private and public encryption keys associated with the destination device [figure 4];

a content encoding key decryptor for decrypting the content encoding key with a content encoding key encryption key [column 12 line 65 to column 13 line 19];

an access card reader for reading an access card, where the access card includes authentication means and a memory which, prior to a first insertion in the destination device, includes at least a second Conditional Access Certificate and a first User Certificate and which, after the first insertion (i.e. receiving the certificate, module 222 verifies that the licensing authority is itself trustworthy. Module 222 verifies that the licensing authority is trustworthy by establishing a "chain" of one or more certificates ranging from the licensing authority up to a root certificate. System 220 maintains a root certificate for each licensing authority that system 220 trusts. Each root certificate is a self-signed certificate that is implicitly trusted by system 220. Upon receipt of the smart card certificate 276, module 220 attempts to establish a chain of certificates from the certificate 276 up to one of the trusted root certificates. This chain may include one or more "intermediate" certificates. Each certificate in the chain will have a "parent" certificate that can cryptographically verify the authenticity of the certificate (e.g., by being digitally signed by the parent). Eventually, the chain leads back to a parent certificate that is one of the trusted root certificates. If such a certificate chain can be established by module 222, then the licensing authority is considered trustworthy. However, if such a certificate chain cannot be established, then the licensing authority is not considered trustworthy and module 222 will not descramble and encrypt the media content.) [column 10, lines 22-43], includes at least the public portion of the private and public encryption keys and which, prior to a subsequent insertion in the destination device, is inserted into a source device and updated to include a content encoding key encrypted with the key encryption key, whereby the destination device, following the subsequent insertion of the access card, has the key encryption key and can decrypt the content encoding key and, using the content encoding key, decode the digital information encoded with the content encoding key [column 12 line 65 to column 13 line 19].

As to claim 9, Marsh discloses a method for securely transferring information from a source device to an external device, the source device having a removable digital memory containing information accessible to the source device, the information contained in the digital memory intended to be protected from unauthorized access, the method comprising:

receiving at the source device user certificate data from an access device and comparing the user certificate data with a first Conditional Access Certificate stored in memory of the source device for authenticating the certificate data (i.e. receiving the certificate, module 222 verifies that the licensing authority is itself trustworthy. Module 222 verifies that the licensing authority is trustworthy by establishing a "chain" of one or more certificates ranging from the licensing authority up to a root certificate. System 220 maintains a root certificate for each licensing authority that system 220 trusts. Each root certificate is a self-signed certificate that is implicitly trusted by system 220. Upon receipt of the smart card certificate 276, module 220 attempts to establish a chain of certificates from the certificate 276 up to one of the trusted root certificates. This chain may include one or more "intermediate" certificates. Each certificate in the chain will have a "parent" certificate that can cryptographically verify the authenticity of the certificate (e.g., by being digitally signed by the parent). Eventually, the chain leads back to a parent certificate that is one of the trusted root certificates. If such a certificate chain can be established by module 222, then the licensing authority is considered trustworthy. However, if such a certificate chain cannot be established, then the licensing authority is not considered trustworthy and module 222 will not descramble and encrypt the media content.) [column 10, lines 22-43];

accessing the information stored in the removable digital memory and encrypting the information stored in the removable digital memory using at least one content encryption key stored in the source device, upon authentication of the certificate data (i.e. The media is encrypted based on smart card 246, thereby requiring smart card 246 to be present in order to decrypt and render the stored content. This decryption and rendering can be performed by any system 220 to which smart card 246 is in communication (e.g., plugged into), such as the system

220 that recorded the content or a system 220 at a friend's house if smart card 246 is taken to the friend's house. Alternatively it can be a physically different smart card, but only if that smart card has the same household identifier stored (securely) inside.) [column 14, lines 15-25];

receiving at the source device a public key from the access device and encrypting the at least one content encryption key using the public key [column 14, lines 15-25]; and

transmitting the encrypted content encryption key to enable access of the encrypted information stored on the removable digital memory by an external device communicable with the access device [column 14, lines 15-25].

As to claim 10, Marsh discloses a method for securely porting digital information from a source device to a destination device comprising:

providing a source device having a removable digital memory and including a first Conditional Access Certificate (i.e. set-top box 242 provides received content 240 that satisfies the conditional access scheme to descrambling and encrypting module 222 via a coupling 244. Set-top box 242 scrambles the content it passes to module 222 in order to prevent a malicious user from tapping into the signal passed between box 242 and module 222 and inappropriately using the content. Coupling 244 can be any of a variety of communications mechanisms, including both wired and wireless. In one implementation, coupling 244 is a USB (Universal Serial Bus) or IEEE 1394 connection) [column 7, lines 11-25];

providing a destination device having a second stored User Certificate and also including mutually corresponding private and public encryption keys associated with the destination device (i.e. Certificate 276 is a certificate that is digitally signed by a trusted licensing authority (also referred to as a certificate authority or certifying authority) testifying that the smart card 246 is authentic. Certificate 276 includes the public key of key pair 270, the public key of the licensing authority, and the above testimony, and is digitally signed by the licensing authority using the private key of the licensing authority. This digitally signed certificate allows module 222, knowing the public key of the licensing authority, to verify that the certificate that is presented by smart card 246 was indeed digitally signed by the licensing authority.) [column 9, lines 57-67];

providing an access card capable of use with both the source device and the destination device, the access card including a second Conditional Access Certificate and a first User Certificate stored therein (i.e. receiving the certificate, module 222 verifies that the licensing authority is itself trustworthy. Module 222 verifies that the licensing authority is trustworthy by establishing a "chain" of one or more certificates ranging from the licensing authority up to a root certificate. System 220 maintains a root certificate for each licensing authority that system 220 trusts. Each root certificate is a self-signed certificate that is implicitly trusted by system 220. Upon receipt of the smart card certificate 276, module 220 attempts to establish a chain of certificates from the certificate 276 up to one of the trusted root certificates. This chain may include one or more "intermediate" certificates. Each certificate in the chain will have a "parent" certificate that can cryptographically verify the authenticity of the certificate (e.g., by being digitally signed by the parent). Eventually, the chain leads back to a parent certificate that is one of the trusted root certificates. If such a certificate chain can be established by module 222, then the licensing authority is considered trustworthy. However, if such a certificate chain cannot be established, then the licensing authority is not considered trustworthy and module 222 will not descramble and encrypt the media content.) [column 10, lines 22-43];

placing the access card in the access card port of the destination device a first time; after the placing of the access card in the destination device a first time, accessing the second User Certificate certificate from the destination device, and, within the access card, authenticating the second User Certificate from the destination device with the second Conditional Access Certificate to determine if the public encryption key should be read from the destination device and stored in the access card; [column 10, lines 22-43]

if the public encryption key of the destination device should be written to the access card, writing the public encryption key from the destination device to the access card [column 10, lines 22-43];

removing the access card from the destination device after the writing of the public encryption key [column 10, lines 22-43];

inserting the access card into the source device, and authenticating the first User Certificate with the first Conditional Access Certificate to determine if the access card is valid;

if the access card is deemed to be valid by the source device, copying the public encryption key from the access card to the source device (i.e. The media is encrypted based on smart card 246, thereby requiring smart card 246 to be present in order to decrypt and render the stored content. This decryption and rendering can be performed by any system 220 to which smart card 246 is in communication (e.g., plugged into), such as the system 220 that recorded the content or a system 220 at a friend's house if smart card 246 is taken to the friend's house. Alternatively it can be a physically different smart card, but only if that smart card has the same household identifier stored (securely) inside.) [column 14, lines 15-25];

at the source device, encrypting at least some of the digital information in the digital memory using at least one content encryption key to produce encrypted information, using the public encryption key from the destination device to encrypt the content encryption key to thereby generate at least one encrypted content encryption key, and storing the at least one encrypted content encryption key in the access card [column 14, lines 15-25];

connecting the port of the digital memory to the digital information port of the destination device [column 12 line 65 to column 13 line 19];

placing the access card in the access card port of the destination device a second time [column 12 line 65 to column 13 line 19];

after the step of placing the access card in the access card port of the destination device a second time, copying the at least one encrypted content encryption key from the access card to the destination device, and decrypting the encrypted content encryption key using the private key information (i.e. The encrypted content is also provided to MPEG decoder module 234. MPEG decoder module 234 decodes (e.g., decompresses) the encoded content (which is encoded in an MPEG format in the illustrated example). Module 234 decrypts the encrypted content prior to decoding the media content, and outputs the decoded content to content renderer module 236. Module 234 can, after decoding the media content, optionally encrypt the decoded content. Whether module 234 encrypts the decoded content is dependent on whether a secure communication channel exists between modules 234 and 236. If there is a secure communication channel (e.g., the modules 234 and 236 are on the same expansion card within system 220, or are within the same display device), then encryption is not necessary. Content renderer module 236 renders the media content via rendering device 294. Although illustrated as a single decoder module 234 and a single renderer module 236, multiple such modules may be included (e.g., one for each type of media content, such as one for audio content and one for video content). Additionally, multiple rendering devices may be included (e.g., one for visual content and another for audio content) [column 12 line 65 to column 13 line 19]; and

at the destination device, receiving the encrypted information from the digital memory, and using the content encryption key to decrypt the encrypted information [column 12 line 65 to column 13 line 19].

As to claim 13, Marsh discloses an access card, the access card comprising:

a memory having at various times at least first, second, and third states (i.e. set-top box 242 provides received content 240 that satisfies the conditional access scheme to descrambling and encrypting module 222 via a coupling 244. Set-top box 242 scrambles the content it passes to module 222 in order to prevent a malicious user from tapping into the signal passed between box 242 and module 222 and inappropriately using the content. Coupling 244 can be any of a variety of communications mechanisms, including both wired and wireless. In one implementation, coupling 244 is a USB (Universal Serial Bus) or IEEE 1394 connection) [column 7, lines 11-25];

authenticating means;

the memory comprising, in the first state, a second Conditional Access Certificate and a first User Certificate stored therein (i.e. receiving the certificate, module 222 verifies that the licensing authority is itself trustworthy. Module 222 verifies that the licensing authority is trustworthy by establishing a "chain" of one or more certificates ranging from the licensing authority up to a root certificate. System 220 maintains a root certificate for each licensing authority that system

220 trusts. Each root certificate is a self-signed certificate that is implicitly trusted by system 220. Upon receipt of the smart card certificate 276, module 220 attempts to establish a chain of certificates from the certificate 276 up to one of the trusted root certificates. This chain may include one or more "intermediate" certificates. Each certificate in the chain will have a "parent" certificate that can cryptographically verify the authenticity of the certificate (e.g., by being digitally signed by the parent). Eventually, the chain leads back to a parent certificate that is one of the trusted root certificates. If such a certificate chain can be established by module 222, then the licensing authority is considered trustworthy. However, if such a certificate chain cannot be established, then the licensing authority is not considered trustworthy and module 222 will not descramble and encrypt the media content.) [column 10, lines 22-43];

the memory, in the second state, following a first insertion of the card and first authentication, where the first insertion of the card is into an access card port of a digital information destination device including digital information port which is capable of receiving the digital information, a second stored User Certificate and mutually corresponding private and public encryption keys associated with the destination device, and the first authentication is performed by the authenticating means authenticating the second User Certificate from the destination device with the second Conditional Access Certificate, comprising the public encryption key from the destination device [column 10, lines 22-43];

the memory, in the third state, following a second insertion of the card and second authentication, where the second insertion of the card is into an access card port of a digital information source device including a removable digital memory containing digital information and a further memory containing a first Conditional Access Certificate and at least one content encryption key, and also following authentication of the first User Certificate stored in the memory of the access card with the first Conditional Access Certificate stored in the source device to establish validity of the access card to the source device, comprising the at least one content encryption key encrypted with the public encryption key (i.e. The media is encrypted based on smart card 246, thereby requiring smart card 246 to be present in order to decrypt and render the stored content. This decryption and rendering can be performed by any system 220 to which smart card 246 is in communication (e.g., plugged into), such as the system 220 that recorded the content or a system 220 at a friend's house if smart card 246 is taken to the friend's house. Alternatively it can be a physically different smart card, but only if that smart card has the same household identifier stored (securely) inside.) [column 14, lines 15-25].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2, 3, 7, 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marsh U.S. Patent No. 7,080,039 B1 as applied to claims 1, 6 and 10 above, and further in view of Roskind et al US 2003/0046544 A1 (hereinafter Roskind).

As to claims 2, 3, 7, 11 and 12, Marsh discloses an access card, as discussed above.

Marsh does not teach means for establishing that the access card is not expired. Marsh does not teach that the means for establishing that the access card is not expired is performed by comparing the current time with a timestamp in the received user certificate data.

Roskind teaches a smart-card [0016] with a digital certificate with an expiration time [0017]. Once the certificate expires, the smart-card becomes useless. Roskin teaches checking these certificates to see if they have expired [0020].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Marsh so that the certificate would have had an expiration time. Once the certificate expired, the smartcard would have become useless. There would have been means for checking to see if the certificate had expired.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Marsh by the teaching of Roskin because the temporary certificates function as a surrogate for the long-term digital certificate and allows the user to immediately remove it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Marsh e the smart card from a card reader and pocket the smart card, thus avoiding the possibility of forgetting the card in a card reader [0012].

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431